THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method of decrypting a message encrypted using a truncated ring cryptosystem, the method comprising the steps of:

   a) selecting a window parameter T determining a plurality of windows of a predetermined size, each window being shifted by an amount less than or equal to the window parameter T;

   b) determining a decryption candidate for each possible window;

   c) testing each decryption candidate to determine whether it is a valid message;

   d) choosing the result of the decryption to be a valid message found in step c or if no valid message is found indicating that the message could not be decrypted;

   whereby a constant number of decryption candidates are determined for each decryption.

2. A method of decrypting a message encrypted using a truncated ring cryptosystem, the method comprising the steps of:

   a) generating a random sequence of integers less than a fixed value, each integer corresponding to a window of a predetermined size and being shifted by the amount of the integer;

   b) successively determining decryption candidates for each possible window, testing the decryption candidates until a valid message is found, and choosing the valid message as the result of the decryption;

   c) if no valid message is found after each possible window is used, indicating that the message could not be decrypted.

3. A method of selecting system parameters for a truncated ring cryptosystem, the method comprising the steps of:

   a) selecting an initial set of parameters;

b) generating private keys;

c) testing the vulnerability of each private key to an attack on the cryptosystem based on determining indecipherable messages;

d) when the cryptosystem is vulnerable, repeatedly increasing the value of one of the parameters and re-testing the vulnerability until the vulnerability has been reduced.

4. A method of encryption with a truncated ring cryptosystem, the method comprising the steps of:

a) using first, second and third cryptographic hash functions to obtain a first string from a message and a number;

b) using said number as a second string;

c) using said first cryptographic hash function to obtain a third string from said message and said number;

d) forming a padded message from said first, second, and third strings;

b) encrypting the padded message with an encryption function.

5. A method according to claim 4, wherein said first string is formed by applying said first hash function to combine said message and said number into a first value, applying said second function to said first value and said number to obtain a second value, and applying said third hash function to said second value and said message to obtain said first string.

6. A method according to claim 5 wherein determining said first value includes concatenating said message and said number.

7. A method according to claim 6, wherein determining said second value includes concatenating said number and said first value.

8. A method according to claim 7, wherein determining said first string includes computing an exclusive or of said message and said second value.

9. A truncated ring cryptographic system comprising:

a) system parameters selected by testing the vulnerability of randomly chosen private keys to an attack based on determining indecipherable messages;

b) an encryption engine;

c) a decryption engine.

10. A truncated ring cryptographic system comprising:

a) system parameters including a window parameter less than 30;

b) an encryption engine;

c) a decryption engine.

11. A truncated ring cryptographic system according to claim 10 wherein said window parameter is less than 10.

12. A truncated ring cryptographic system according to claim 11 wherein said window parameter is 3.

13. A truncated ring cryptographic system according to claim 11, wherein said window parameter is 2.

14. A truncated ring cryptographic system according to claim 11, wherein said window parameter is 1.

15. A decryptor for a truncated ring cryptographic system comprising:

a) a window parameter T determining a plurality of windows of a predetermined size, each window being shifted by an amount less than the window parameter T;

b) a calculator to determine a decryption candidate for each possible window;

c) a tester to determine whether each decryption candidate is a valid message;

d) a selector to choose the result of the decryption to be a valid message found in step c or if no valid message is found indicate that the message could not be decrypted.

16. A decryptor for a truncated ring cryptographic system comprising:

a) a random sequence of integers less than a fixed value, each integer corresponding to a window of a predetermined size and being shifted by the amount of the corresponding integer;

b) a calculator to determine a decryption candidate for each possible window;

c) a tester to determine whether each decryption candidate is a valid message;

d) a selector to choose the first valid message found by the tester as the result of the decryption.

17. A system parameter selector for a truncated ring cryptographic system comprising:

a) an initial set of parameters;

b) a private key generator;

c) an attack engine to determine the vulnerability of each private key to an attack on the cryptosystem based on determining indecipherable messages;

d) a parameter updater to repeatedly increase the value of one of the parameters and run the attack engine until the vulnerability of the system to the attack has been reduced.

18. An encryptor to encrypt a message in a truncated ring cryptographic system comprising:

a) a first, a second, and a third cryptographic hash function;

b) a generator to generate a number;

c) a message padder configured to form a padded message from a first string computed using said first, second and third cryptographic hash functions on said message and said number, a second string formed from said number and a third string computed using said first cryptographic hash function on said message and said number;

d) an encryptor to encrypt said padded message using an encryption function.

19. An encryptor according to claim 18, wherein said first string is formed by applying said first hash function to combine said message and said number into a first value, applying said second function to said first value and said number to obtain a second value, and applying said third hash function to said second value and said message to obtain said first string.

20. An encrytor according to claim 19 wherein combining said message and said number into said first value includes concatenating said message and said number.

21. An encryptor according to claim 20, wherein obtaining said second value includes concatenating said number and said first value.

22. An encryptor according to claim 21, wherein obtaining said first string includes computing an exclusive or of said message and said second value.

23. A data carrier containing instructions to direct a processor to decrypt a message encrypted using a truncated ring cryptosystem, the data carrier including instructions to:

a) select a window parameter T determining a plurality of windows of a predetermined size, each window being shifted by an amount less than or equal to the window parameter T;

b) determine a decryption candidate for each possible window;

c) test each decryption candidate to determine whether it is a valid message;

d) choose the result of the decryption to be a valid message found in step c or if no valid message is found indicating that the message could not be decrypted;

whereby a constant number of decryption candidates are determined for each decryption.

24. A data carrier containing instructions to direct a processor to decrypt a message encrypted using a truncated ring cryptosystem, the data carrier including instructions to:

a) generate a random sequence of integers less than a fixed value, each integer corresponding to a window of a predetermined size and being shifted by the amount of the integer;

b) successively determine decryption candidates for each possible window, test the decryption candidates until a valid message is found, and choose the valid message as the result of the decryption;

c) if no valid message is found after each possible window is used, indicate that the message could not be decrypted.

25. A data carrier containing instructions to direct a processor to select system parameters for a truncated ring cryptosystem, the data carrier including instructions to:

a) select an initial set of parameters;

b) generate private keys;

c) test the vulnerability of each private key to an attack on the cryptosystem based on determining indecipherable messages;

d) when the cryptosystem is vulnerable, repeatedly increase the value of one of the parameters and re-test the vulnerability until the vulnerability has been reduced.

26. A data carrier containing instructions to direct a processor to encrypt a message using a truncated ring cryptosystem, the data carrier including instructions to:

a) use first, second and third cryptographic hash functions to obtain a first string from a message and a number;

b) use said number as a second string;

c) use said first cryptographic hash function to obtain a third string from said message and said number;

d) form a padded message from said first, second, and third strings;

b) encrypt the padded message with an encryption function.

27. A data carrier according to claim 26, wherein said first string is formed by applying said first hash function to combine said message and said number into a first value, applying said second function to said first value and said number to obtain a second value, and applying said third hash function to said second value and said message to obtain said first string.

28. A data carrier according to claim 27 wherein determining said first value includes concatenating said message and said number.

29. A data carrier according to claim 28, wherein determining said second value includes concatenating said number and said first value.

30. A data carrier according to claim 29, wherein determining said first string includes computing an exclusive or of said message and said second value.